Aspectos Gerais de Forense Computacional - Unisinos

Victor Hugo Menegotto
vmenegotto@axur.com.br

Forense Computacional

» **Victor Hugo Menegotto**

- Consultor de Segurança da Informação da Axur Information Security
- 7 anos em Tecnologia da Informação
- Atendeu 10 das 20 maiores empresas da região sul
- No último ano realizou mais de 20 processos de investigação
- Vice-presidente do IISFA - International Information Systems Forensics Association

O que é Segurança da Informação?

» Hackers estrangeiros capturando números de CC
» Websites de grandes corporações sendo desfigurados por razões políticas
» Ataques de vírus que paralisam grandes corporações
» Espiões digitais capturando e vendendo informações sobre concorrentes e gigantescos bancos de dados

Forense Computacional

Cenário Nacional

» Incidentes de segurança da informação crescem 117% em 2003 (54.607 incidentes em 2003 x 25.092 em 2002)

» Fraudes: aumento de 498% em 2003.

» As primeiras ações geradas após um incidente de segurança acabam prejudicando o processo de investigação e de perícia

Forense Computacional

Cenário Nacional

» "Brasil é líder mundial em crimes na Internet"
(Folha de SP – 20/11/02)

» Levantamento da consultoria britânica mi2g (FBI Computer Crime and Security Survey, CNN, BBC, Time):

- » Brasil é o maior originador de ataques
- » Os dez grupos de hackers mais ativos no mundo são brasileiros
- » Brasil é segundo maior alvo de ataques

Forense Computacional

Cenário Nacional: Crimes Comuns

- » Envio de informações confidenciais por e-mail
- » Ataque ou tentativa de ataque por concorrentes
- » Ataque ou tentativa de ataque por funcionários
- » Fraude em sistemas financeiros (home banking)
- » Instalação de cavalos-de-tróia em estações de trabalho
- » Envio de ameaças por e-mail
- » Remoção ou alteração indevida de informações
- » Ataques contra a disponibilidade de sistemas

Forense Computacional

Hackers: Personagens Famosos

» **Vladimir Levin (Rússia):**

Preso pela Interpol após meses de investigação, nos quais ele conseguiu transferir 10 milhões de dólares de contas bancárias do Citibank. Insiste na idéia de que um dos advogados contratados para defendê-lo é (como todo russo neurótico normalmente acharia), na verdade, um agente do FBI. Ele não é tão feio quanto parece nesta foto.

Forense Computacional

Hackers: Personagens Famosos

» **Mark Abene (EUA):**

Inspirou toda uma geração a fuçar os sistemas públicos de comunicação - mais uma vez, a telefonia - e sua popularidade chegou ao nível de ser considerado uma das 100 pessoas mais "espertas" de New York. Trabalha atualmente como consultor em segurança de sistema.

Forense Computacional

Hackers:
Personagens Famosos

» **Kevin Poulsen (EUA):**

Amigo de Mitnick, também especializado em telefonia, ganhava concursos em rádios. Ganhou um Porsche por ser o 102º ouvinte a ligar, mas na verdade ele tinha invadido a central telefônica, e isso foi fácil demais.

Forense Computacional

Hackers:
Personagens Famosos

» **Kevin Mitnick (EUA):**

O mais famoso hacker do mundo. Atualmente em liberdade condicional, condenado por fraudes no sistema de telefonia, roubo de informações e invasão de sistemas. Os danos materiais são incalculáveis.

Forense Computacional

Hackers: Personagens Famosos

» **Robert Morris (EUA):**

Espalhou "acidentalmente" um worm que infectou milhões de computadores e fez boa parte da Internet parar em 1988. Ele é filho de um cientista chefe do National Computer Security Center, parte da Agência Nacional de Segurança. Ironias...

Forense Computacional

Hackers: Personagens Famosos

» **John Draper (EUA):**

Praticamente um ídolo dos três acima, introduziu o conceito de Phreaker, ao conseguir fazer ligações gratuitas utilizando um apito de plástico que vinha de brinde em uma caixa de cereais. Obrigou os EUA a trocar de sinalização de controle nos seus sistemas de telefonia.

Forense Computacional

Hackers: Personagens Famosos

» **Johan Helsingius (Finlândia):**

Responsável por um dos mais famosos servidores de email anônimo. Foi preso após se recusar a fornecer dados de um acesso que publicou documentos secretos da Church of Scientology na Internet. Tinha para isso um 486 com HD de 200Mb, e nunca precisou usar seu próprio servidor.

Forense Computacional

O que é *Forensics*?

» **Forensics:** ciência, dividida em diversas disciplinas, que atua em conjunto com o investigador na busca pela verdade. O AAFS (American Academy of Forensic Sciences), possui os seguintes comitês:

- Criminalistica
- Engenharia
- Jurisprudência
- Odontologia
- Patologia/Biologia
- Antropologia
- Psiquiatria
- Toxicologia
- Endocrinologia
- Computacional

O que é Forense Computacional?

» Forense computacional compreende a aquisição, a preservação a identificação, a extração, a restauração, a análise e a documentação de evidências computacionais.

» Este processo permite o rastreamento, identificação e comprovação da autoria de ações não autorizadas como violações de normas internas e até mesmo crimes eletrônicos.

Forense Computacional

Computer Forensics History

» Evidências derivadas de computadores aparecem nos tribunais por aproximadamente 30 anos

» Com o avanço da tecnologia surgiu a necessidade de tratamento especial para este tipo de evidência

» Em 1976 foi criado o US Federal Rules of Evidence que abrange alguns aspectos

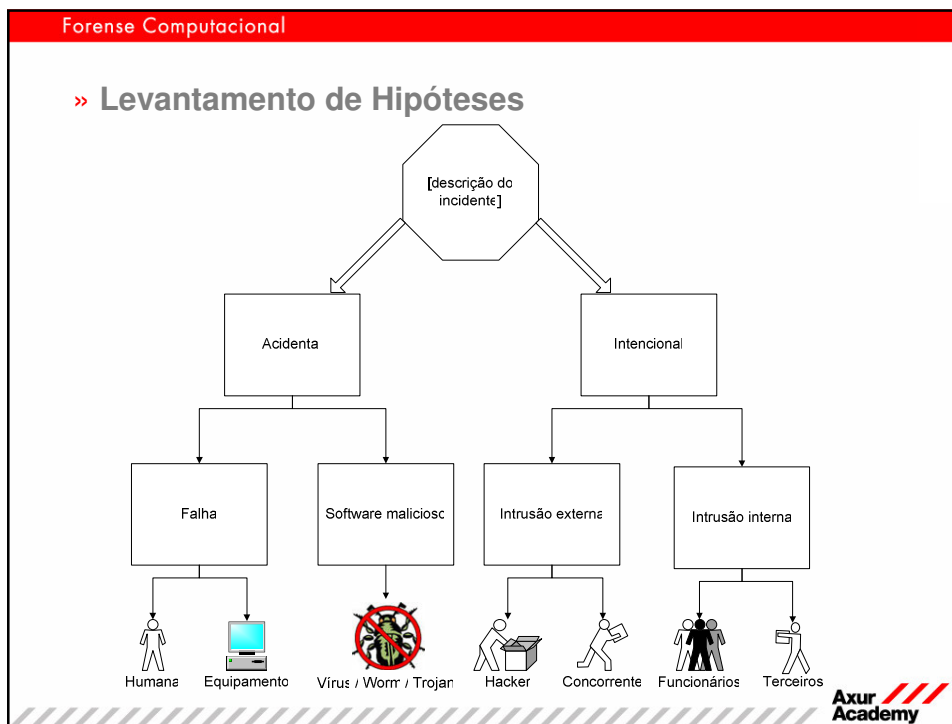
» Outras leis foram desenvolvidas, mas ainda sim, a evolução de alguns aspectos se faz necessária

Desenvolvendo uma Investigação

Desenvolvimento da Investigação

» **Análise do Ambiente**
Organizar os passos a serem dados, evitando interrupções. Qualquer informação informal deve ser registrada em ata de entrevista.

» **Identificação de Hipóteses**
Analisar e avaliar as possibilidades de como o incidente pode ter ocorrido (hipoteses).

Forense Computacional
» Levantamento de Hipóteses
[descrição do incidente]
Acidenta
Intencional
Falha
Software malicioso
Intrusão externa
Intrusão interna
Humana
Equipamento
Vírus / Worm / Trojan
Hacker
Concorrente
Funcionários
Terceiros
Axur Academy

Forense Computacional
Desenvolvimento da Investigação
» Salvaguarda do Ambiente
O ambiente deve ser cuidadosamente protegido, evitando acessos indevidos durante o processo de investigação – md5, imagem...
» Coleta de Evidências
As evidências coletadas devem auxiliar o processo de investigação, contribuindo para a corroboração ou rejeição das hipóteses.
Axur Academy

Forense Computacional

Desenvolvimento da Investigação

» **Análise do Incidente**
Avaliar todos os aspectos referentes ao tipo e a forma de realização do "ataque". Tentar reconstituir o incidente.

» **Análise de Ativos Envolvidos**
Todos os ativos envolvidos devem ser analisados – computadores, disquetes, CDs...

Forense Computacional

Desenvolvimento da Investigação

» **Análise Gerencial**
Analisar registros de segurança dos sistemas que possuam qualquer relação e/ou possam auxiliar no processo de investigação – logs de aplicações, documentos, vídeos de segurança...

» **Traceback**
Realizar buscas e tentar identificar a origem dos ataques – ISPs, empresas, cable modem, ADSL...

Requerimentos

Quem vai ser envolvido?

- Dependerá do tipo de análise:
  - Auditoria Interna
  - Área de Rede e Operações
  - Security Officer
  - Segurança Física
  - Recursos Humanos
  - Legal / Compliance
  - Consultores Externos

Geração de Relatórios

- **Análise de Evidências**

As evidências coletadas devem ser analisadas e correlacionadas com as hipóteses levantadas.

- **Geração de Relatórios**

Agrupamento de todos os aspectos avaliados e conclusão.

Forense Computacional

Geração de Relatórios

» **Investigação litigiosa e não litigiosa**
O tipo de investigação é extremamente importante, não somente ao processo, mas também para a confecção dos relatórios.

» **Linguagem dos relatórios**
Dependendo do tipo de análise, a linguagem dos relatórios pode, ou não, ser técnica. O acerto de expectativas e objetivos é realizado no início do processo de investigação.

Forense Computacional

Geração de Relatórios

- Sumário Executivo
  - Objetivos
  - Descrição do evento
  - Metodologia utilizada
  - Breve descrição das evidências e hipóteses
- Apresentação detalhada das hipóteses
- Apresentação das evidências

- **Conclusão**

CENÁRIO			Falha - Acidental		Ação de Software Malicioso	Intrusão Externa		Intrusão Interna		CONSOLIDAÇÃO Nome EM xx/xx/xxxx		Classificação da Evidência										
HIPOTESES			Primeira Hipotese - Falha Humana - Não Intencional	Segunda Hipotese - Falha no Equipamento (em Software ou Hardware)	Terceira Hipotese - Ação de Software Malicioso - Virus, Worm ou Trojan	Quarta Hipotese - Ação de Hacker	Quinta Hipotese - Ação de Concorrente	Sexta Hipotese - Ação Intencional de Funcionário	Sétima Hipotese - Ação Intencional de Terceiros / Prestadores de Serviço Interno			Best Evidence	Secondary Evidence	Direct Evidence	Conclusive Evidence	Circumstancial Evidence	Opinion Evidence - Expert	Hearsay Evidence	Hearsay Evidence (pontuação: 0 - baixo; 2 - médio; 4 - alto)			
N	EVIDÊNCIAS	EVIDENCE OWNER/ASSET								PONT.	COLETOR/ENTREVISTADOR								CONFIAVEL	SUFICIENTE	RELEVANTE	Σ
1										0												0
2										0												0
10										0												0
11										0												0
	PONTUAÇÃO		0	0	0	0	0	0	0													

Sorteio de Vaga para Curso:

» Responda a pergunta:

"Por que eu quero participar do curso Forense Computacional?"

Enviar respostas + currículo e telefone para contato até dia 02/12 às *17hs* para: curriculos@axur.com.br

Resultado na web dia 03/12 às 15hs
www.axur.com.br

Próximos Cursos:
www.axur.com.br/academy

///AXUR ACADEMY

Muito Obrigado!

Victor Hugo Menegotto
vmenegotto@axur.com.br

IISFA – International Information Systems Forensics Association

Victor Hugo Menegotto
vmenegotto@axur.com.br

O que e o IISFA?

» Principal associação mundial da comunidade de forense computacional

» Criada para satisfazer a necessidade de uma referência para a criação e difusão de conteúdo confiável sobre Segurança da Informação, referendado por especialistas

» Composto por diversos profissionais de segurança, de setores públicos e privados, incluindo: consultores de segurança, gerentes de tecnologia, advogados, analistas de sistemas, segurança patrimonial, inteligência e contra-inteligência, estudantes, entre outros

Forense Computacional

Objetivos do IISFA Brasil:

» Difundir a cultura de forense computacional no Brasil
» Fornecer informação para profissionais de TI e outras áreas
» Trocar conhecimento e experiências
» Equalizar conceitos e entendimentos
» Ser referência nacional no tema
» Certificar profissionais CIFI no Brasil
» Contribuir para tornar o Brasil uma referência internacional nesse tema

Forense Computacional

CIFI:

» "*Certified Information Forensics Investigator*"

» Certificação independente para profissionais de forense computacional. Certifica os seguintes domínios:
- » Auditoria
- » Controles de Segurança
- » Técnicas de Forense Computacional
- » Resposta a Incidentes
- » Investigação e Aspectos Legais
- » *Traceback*

» Requer adesão a um rígido código de ética

Por que participar do IISFA?

» Desenvolvimento profissional: workshops, seminários, grupos de estudo e treinamentos

» Networking: Oportunidade de conhecer, trocar idéias e experiências com diversos profissionais de segurança

» Reconhecimento: Ser pioneiro nessa indústria. Tornar-se interlocutor para compartilhar experiências e melhores práticas em uma das áreas que mais crescem no mercado.

Forense Computacional

Links Úteis:

IISFA World Site: www.iisfa.org

NIC BR Security Office: www.nbso.nic.br

Comitê Gestor Internet Brasil: www.cg.org.br

Security Focus: www.securityfocus.com

IISFA – International Information Systems Forensics Association

Victor Hugo Menegotto
vmenegotto@axur.com.br